Chapter 2

1. Secure Programs

بنعتبر اى برنامج انه سيكيور لو قدر يحقق اهداف السيكيورتى الى اتكلمنى عليها فى Chapter1 فبيكون

-enforces the expected security goals
-takes too long time to break
-it runs for a period of time without failures

trust كل ده بيجعله على درجة كبيره من الثقه

2-Way to assess security or quality is to ask people to name the characteristics of Software that Contribute to its overall security

هنا بيقول ازاى اقيم البرنامج بتاعى لو هوا سيكيور ولا لا فيه طريقه انك ممكن تسال المستخدمين الى هيدوك ايجابات مختلفه عن رايهم لانهم بيكونا بصين على quality وال usability وكمان لو حصل فيه faults ولا لا

كل ده لانى انا بكون خايف ان ال attacker يركب كود على البرنامج بتاعى ويشغل حاجه تانيه زى مثلا المشههور اوى انه يخلى الجهاز بتاعك يكون FTP SERVER فمنهنا جهازك بقى خادم الى رايح والى جاى يخش عليه وكمان عايز احمى البرنامج بتاعى من theft وعايز اطول long LIFE TIME بتاعه يشتغل اطول وقت من غير ما ال attacker يقدر يلعب او يوقف ال availability بتاع البرنامج زى البرنامج الى بيقعد ٣٠ يوم وكدا ازاى احميه بان محدش يقدر يهاك عليه ويزود٣٠ او يلغيها

2-Program faults:

هنا بقه طريقه تانيه ممكن استغلها واعمل اتاك ان يحصل فى البرنامج Errors هنا انا ممكن استغل ال errorده واعمل الى انا عيزه فيه نوعين :

Faults:

Fault: An incorrect step, command, process or data definition in a piece of software.

دى بتكون Unexpected Error مشكله فى البرنماج غير متوقعه زى لو انته بتلعب لعبه مثلا ووقفت وجالك رساله بتقول RUN ERROR NUMBER 523 فهنا فى برامج بتستغل الخطا ده وتقدر تخش على الكود ويكون متاح ليك وتعمل اتاك او تسرقه وتعيش بقه

Failures:

هنا بقه البرنامج كله بيقف وكمان ممكن تكون ليه درجه من التدمير يسقط النسخه يدمر بيانات فى الميمورى او يخرب الجهاز كله وده اخطر بك

Failure:A departure from the system's desired behaviour.

Note that:
- An error may cause many faults.
- Not every fault leads to a failure. مش اى خطا ممكن يقفل او يوقف البرنامج ويادى الى دمار النظام كله

Error:A human mistake in performing some software-related activity, such as specification or coding.

Basic Ideas

هنا الفكره اخطاء او عيون اى برنامج او سلوك غير متوقع منه

- A **program security flaw**is an undesired program behavior caused by aprogram vulnerability.

- Work on program security considers two questions:

- How do we keep programs free from flaws?
- How do we protect computing resources against programs with flaws?
- Early idea was to attack the finished program to reveal **faults**, and then to patch the corresp. **errors**.
- Experience shows that this is not effective, and just tends to introduce new faults (and errors)!
- More modern approach is to use careful specification and compare behavior with the expected.

Program security flaws

عيوب اى برنامج ممكن يحصله اتاك عن طريقه ليهم نوعين .
انواع ال FLAWS

1. **Non-malicious flaws**. Introduced by the programmer overlooking something:
- Buffer overflow
- Incomplete mediation
- Time-of-check to Time-of-use (TOCTTU) errors

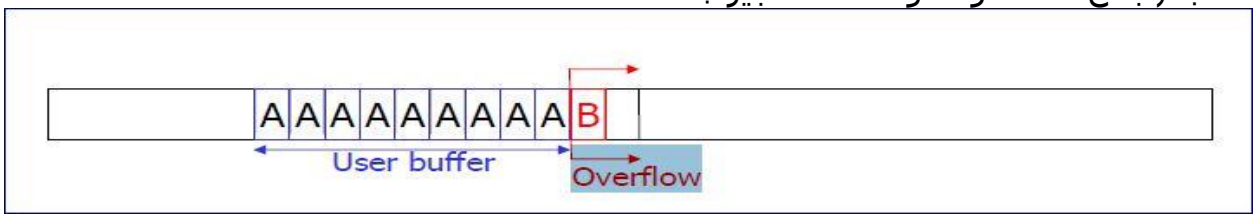
ده اول نوع عندنا بيتسبب بابن الذكيه programmer نفسه نتكلم على انواعه بقه

Buffer overflow:

A program that fails to check for buffer overflow may allow vital data or code to be overwritten:

هنا بقه يعنى انته عملت مثلا مصفوفه عملت Control على Size بتاعها
فثبت حجمها طبعا بيروح Compiler فى الميمورى يحجز الحجم ويكون المكان
ده مكان User –Buffer ١٠الى ٩ مثلا المشكله لو سيتك دخلت او البروجرامر

دخل arr[10] دخل ليها قيمه هنا بقه انته عملت Overflow يعنى عديت الحجم بتاع المصفوفه وده خطا كبير جدا



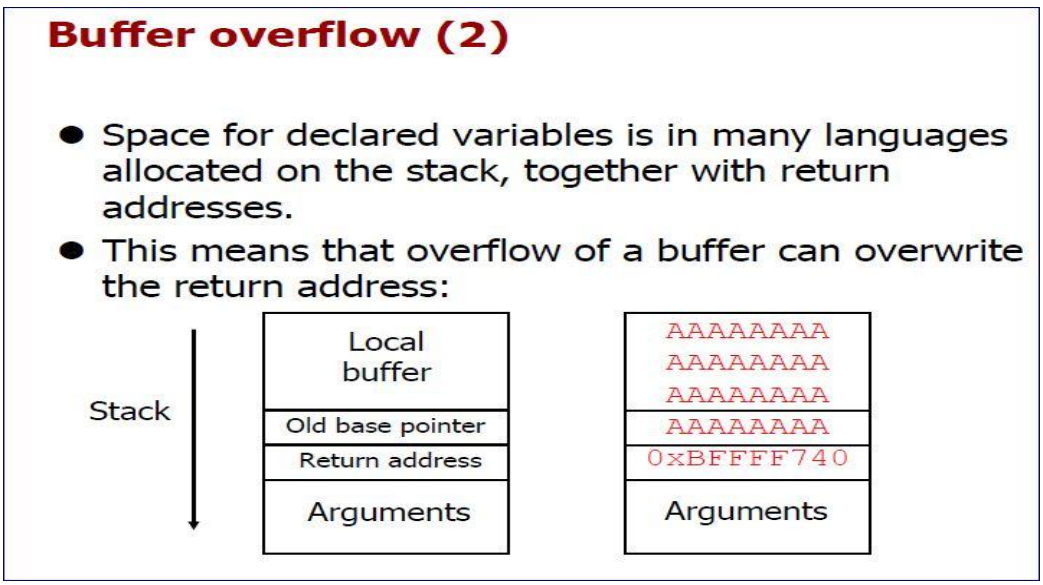
طيب ممكن ياثر او يدمر ايه حاجه زى دى او اخاف منها فى ايه.

Buffer may overflow into (and change):

- User's own data structures ممكن يغير فى الداتا
- User's program code فى البرنامج بتاعك نفسه ويدمره
- System data structures السيستم نفسه هباااا هنا بقه المشكله الداتا لل
- System program code وكمان البرامج بتاعت ال

والاخطر انك ممكن تعمل overflow على return address الى فى الاستاك زى ما احنا عرفين ان الميمورى فيها استاك وهيب

وكمان فى بعض الاحيان تشغل برنامج مره يشتغل والتانيه يترخم وميشتغلش لانه بيكون معتمد على الميمورى وال buffer overflows



Buffer overflow in ASP

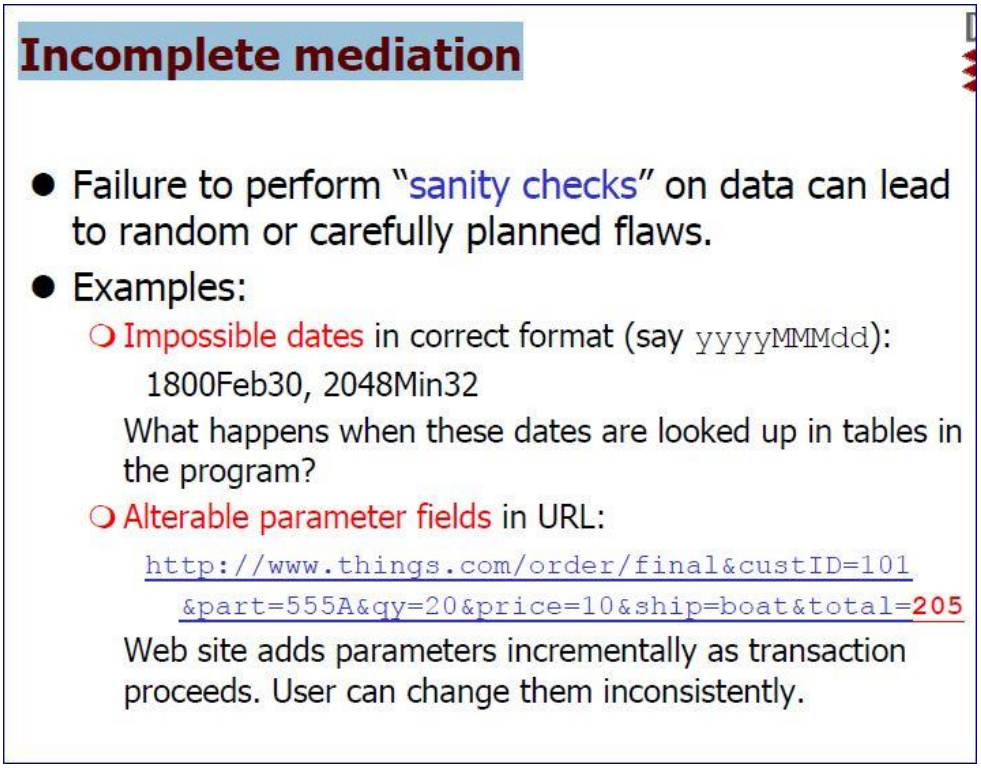
-loop (response.redirect();)

-scripting (internet explorer not allow Java script)

-phone number

Incomplete mediation

زى لما اكتب التاريخ بالطريقه دى ٢٠٠٩/١٢/١ هنا تروح للداتا طيب لو كان الداتا شغاله شهر /يوم / سنه هيحصل عندك مشكله كبيره فالحل هنا فى design انك متسمحشى لليوزر يدخل بمزاجه تعملوا مثلا dropdown listفيها اليوم او CompoBox والتاريخ والسنه ويختار منهم



Time-of-check to Time-of-use (TOCTTU)

A **delay** between checking permission to perform certain operations and using this permission may enable the operations to be changed.

هنا بيفرق بين وقتين وقت التاكدمن صحة المعلومات عشان يسمحلك بالدخول زى الاله العبقريه الى موجوده فى مصر ِ ATM هنا بقه لما تدخل الكرت ويسالك اساله كتير وغريبه فهنا بيزود وقت ال time of check عشان يقدر يدخلك على الداتا وطبعا ده خطر يعنى ممكن بعد لما دخلت الباسورد والكارت وقعد يعملك فحص لوقت طويل ممكن حد يضربك على دماغك مثلا مثلا يعنى ويخش بقه ويعيش ويا خد الفلوس الى هوا عيزها لانك كنت دخلت الباسورد والكارت

مثلا تانى عليها بس برمجى شويه

Example:
1. User attempts to write 100 bytes at end of file “abc”. Description of operation is stored in a data structure.
2. OS checks user’s permissions on copy of data structure.
3. While user’s permissions are being checked, user changes data structure to describe operation to delete file “xyz”.

بيجى للنوع التانى بقه من ال FLAWS
Malicious CODEالبرامج الخبيثه

Malicious code

DTU

- **Virus:** Attaches itself to program or data, passing malicious code on to non-malicious programs by modifying them.
- **Trojan horse:** Has non-obvious malicious effect in addition to its obvious primary effect.
- **Logic/time bomb:** Has malicious effect when triggered by certain condition.
- **Trapdoor/backdoor:** Gives intruder (possibly privileged) access to computer.
- **Worm:** Stand-alone program which spreads copies of itself via a network.
- **Rabbit:** Reproduces itself continually to exhaust resources.

ودى سهله بس افضل تتقرا من الكتاب لانها معموله فى مجموعة جداول جميله وبسيطه

نيجى بقه لانواع Virus يعفينا ويعفيكوا يارب

1-Document Virus

طبعا ده اخطرهم لانك مبتشوفوش Attached to(NOTE BADE ,Office Word, Image)

Virus Code: Executable Code Attached To the Program

2- Virus Appended To a program

هنا بقه بيكون البرنامج معموله execution عن طريق الفيرس هيشتغل معاه كمان لانه بيبقى كود مضاف الى البرنامج الاصلى فال control هيتحول بقدرة قادر من original program الى virus طبعا بيبقى ليه جمل calling معينه وكمان ليه جمل execution بيتنقل بيها بس سهل على اى anti-virus انه يمسكه او يكتشفه لانه بيبقى فى اول الكود بتاع البرنامج وعادتا جمل calling وال execution بتاع انواع كتيره من الفيرس بتبقى معروفه او مالوفه فال anti-virus لما يشوفها يعرفها على طول طبعا مننساش ان جمل execution هيا الى بتنقل ال controlمن البرنامج الاصلى الى الفيرس الرسمه فى الكتاب صفحة ٢-٣٦

3-serrounded virus

من اسمه يحيط البرنامج من كل جوانبه يعنى هيبقى فى اول الكود واخره والمشكله هنا ان anti-virus هيشوف الجزء الاول فوق و التانى مش هيشوفه

4-Modified Program Virus (integrated Virus)

من اسمه بردك هنا يعنى اتعدل معاهيعنى مثلا خلينا مشين بطريقة interpreter زى php سطر بسطر هنا بقه الفيرس مش هيكون جزء واحد او جزئين ده هيكون مندمج مع البرنامج نفسه يعنى ممكن تلاقى سطر كود للبرنامج والتانى للفيرس بدون دخول فى تفاصيل كتيره تعبير مجازى

طبعا هنا anti-virus مش هيكون عنده الا حل واحد انه يشيل البرنامج ده لو anti-virus غبى شويه زى AVAST القديم

طبعا المفرود زى *Avira* انه بيشوف هل ده هيضر ال system ولا لا لو هيضره انه يشيله فالحل انه بيعمله حاجه اسمها freezing بيجمده او

How Virus Gain Control?

قبل لما نتكلم لازم نعرف حاجه اسمها ال pointer والحاجه دى هيا الى بقدر اقرا او هيا الى بتقرا فى الميمورى مباشر يعنى بتبقى UNSAFE كود زى ما اخدنا فى تشفير الصوره فى السيكشن

اول نوع عندنا فى جمل ال execution الى الفيرس هياخد ال control من البرنامج ويضحك عليه هيا

1-overwriting

هنا الطريقه الاولى بص فى السمه الى فى الكتاب صفحة ٢-٤١

اول حاجه عندك directory File فيه الكود وكدا وكمان فيه حاجه اسمها target File لما البوينتر يمشى عليه ويلاقى ال target file هنا بقه المفروض ينفزه لا هنا بيجى يقراه يلاقى انه virus وبيشاور على virus

2-changing Pointer

الطريقه التانيه بقه انك هنا البوينتر المفروض يروح على target file هنا الفيرس حاتط جمل jump زى :GO TO aa

الى اخدناها فى البرمجه فلما يجى يقرا ال target file يلا الجمله دى يقوم متحول من ال target file الى virus ويقرا ملف الفيرس فهنا غيرت pointer

الحل هنا anti-virus انه يلاقى جمل ال callingو jump دى ويمسحها طبعا مش كلها بتبقى فيه جمل غريبه مختلفه عن سياق الكود بتاع البرنامج الاصلى زى برنامج بيجمع رقمين تلاقى فيه jump لمف shutdown فى النظام بتاعك وكمان جمل ال execution بتبقى معرفه انها للفيرس

نيجى لاخر جاه بقى حاجه اسمها boot sector Virus

هنا بقه خشينا فى virusالى ملوش حل ايوه ملوش حل هما اتنين ده اولهم

نتكلم عنه فى جزء لما تيجى الشركه المصنعه للهارد وير تربط الهارد بال سوفت وير او firmware الى هوا os بتصنح حاجه اسمها boot sector ده بيكون protected highly

بيكون connected with ur pc

بيجيله فيرس ازاى .

المفروض لما تشغل جهازك بيكون عندك بيوينتر فى boot sector المفروض يتنقل الى الميمورى لان الميمورى بيكون فيها code بيقول انه يقرا OS من على الهارد بتاعك الى هوا فهنا الفيرس بيخلى pointer

يروح لحته تانيه فيخلى OS يفضل يموت او الجهاز يجى يشغل osتلاقيه يرستر كل شويه لانه مش قادر يوصله

التانى بقه Memory –Resident Virus

هنا بقه بيقول انه فيه برامج بتاخد وقت كتير لما تفتح صح فاحنا بقه بنخليها تفتح لما os يعمل start UP زى yahoo NetCUTوكدا طيب ازاى اتفتحت ولسه الجهاز بيقوم

هنا بقه الشكله

ليها كود موجود فى الميمورى حتى من الاسم resident code in memory فبيكون عندك على desktop ايكون بس بتتكه عليه بيعمل callingللكود الى فى الميمورى فهنا بقه المشكله لو البرنامج ده فيه فيرس هيشتغل اول ما السيستم يقوم قبل ما حتى ال anti-virus يقوم فهنا بيبقى ملوش حل الى الان وهيشتغل معاه علطول

طبعا بقى بس virus signature

هيا ان الفيرس بيكون ليه اثر او امضاء بتبينه كل جريم هليها دليل

ده والله الى انا فهمه على قدى لو اى حد عايز يزود او يعدل يا ريت والله

شكرا

Eng. Mohamed Ibrahim